REMARKS

The Examiner is thanked for the thorough examination of the present application. The Office Action mailed December 20, 2006 rejected claims 1-124. This is a full and timely response to that outstanding Office Action. Upon entry of the amendments in this response, claims 1-124 are pending. More specifically, claims 1, 24, 38, 55, 69, 77, 83, 92, 100, 105, 110, 115, and 120 are amended. These amendments are specifically described hereinafter.

I. Present Status of Patent Application

Claims 1-124 are rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. These rejections are respectfully traversed.

II. Rejections Under 35 U.S.C. §103(a)

A. Claims 1-23

The Office Action rejects claims 1-23 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 1, as amended, recites:

> 1. A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver;
>
> ***applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

(Emphasis added).

Applicant respectfully submits that claim 1 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue. *See, e.g., In re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988) and *In re Keller*, 208 U.S.P.Q.2d 871, 881 (C.C.P.A. 1981).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the

3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 1, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 1 is allowable over the cited references of record, dependent claims 2-23 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that dependent claims 2-23 contain all the features of independent claim 1. *See Minnesota Mining and Manufacturing Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002) *Jeneric/Pentron, Inc. v. Dillon Co.*, 205 F.3d 1377, 54 U.S.P.Q.2d 1086 (Fed. Cir. 2000); *Wahpeton Canvas Co. v. Frontier Inc.*, 870 F.2d 1546, 10 U.S.P.Q.2d 1201 (Fed. Cir. 1989). Therefore, the rejection to claims 2-23 should be withdrawn and the claims allowed.

B. Claims 24-37

The Office Action rejects claims 24-37 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 24, as amended, recites:

> 24. A method for securely providing in a subscriber network encrypted programming, which is received at a receiver at a subscriber location, the encrypted programming includes a plurality of ciphertext packets, and wherein the subscriber network includes a headend for distributing the encrypted programming and a plurality of receivers including the receiver at the subscriber location, at the headend the method comprising the steps of:
>
> applying to a cleartext packet a first cryptographic algorithm to convert the cleartext packet to a first ciphertext packet;
>
> transmitting the first ciphertext packet to the receiver; and
>
> at the receiver the method comprising the steps of:
>
> receiving the first ciphertext packet;
>
> ***applying to the first ciphertext packet a second cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> applying to the second ciphertext packet a third cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

(Emphasis added).

Applicant respectfully submits that claim 24 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 24 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying to the first ciphertext packet a second cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least

one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 24, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 24 is allowable over the cited references of record, dependent claims 25-37 (which depend from independent claim 24) are allowable as a matter of law for at least the reason that dependent claims 25-37 contain all the features of independent claim 24. Therefore, the rejection to claims 25-37 should be withdrawn and the claims allowed.

C. Claims 38-54

The Office Action rejects claims 38-54 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 38, as amended, recites:

> 38. A receiver in a subscriber network that receives encrypted programming, from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first ciphertext packet of the encrypted programming;
>
> a key generator adapted to generate a plurality of encryption keys; and
>
> ***a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm at least twice using at least one encryption key and the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.***

(Emphasis added).

Applicant respectfully submits that claim 38 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 38 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm at least twice using at least one encryption key and the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting

the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 38, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 38 is allowable over the cited references of record, dependent claims 39-54 (which depend from independent claim 38) are allowable as a matter of law for at least the reason that dependent claims 39-54 contain all the features of independent claim 38. Therefore, the rejection to claims 39-54 should be withdrawn and the claims allowed.

D. Claims 55-68

The Office Action rejects claims 55-68 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 55, as amended, recites:

> 55. A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver; and
>
> ***applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***.

(Emphasis added).

Applicant respectfully submits that claim 55 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 55 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one

embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 55, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 55 is allowable over the cited references of record, dependent claims 56-68 (which depend from independent claim 55) are allowable as a matter of law for at least the reason that dependent claims 56-68 contain all the features of independent claim 55. Therefore, the rejection to claims 56-68 should be withdrawn and the claims allowed.

E. Claims 69-76

The Office Action rejects claims 69-76 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 69, as amended, recites:

> 69. A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, at the headend the method comprising the steps of:
>
> receiving a first ciphertext packet;
>
> ***applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***;
>
> transmitting the second ciphertext packet; and
>
> at the receiver the method comprising the steps of:

receiving the second ciphertext packet having multiple layers of encryption thereon; and

applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a third ciphertext packet without first convering the second ciphertext packet to a cleartext packet.

(Emphasis added).

Applicant respectfully submits that claim 69 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 69 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited

combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 69, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 69 is allowable over the cited references of record, dependent claims 70-76 (which depend from independent claim 69) are allowable as a matter of law for at least the reason that dependent claims 70-76 contain all the features of independent claim 69. Therefore, the rejection to claims 70-76 should be withdrawn and the claims allowed.

F. Claims 77-82

The Office Action rejects claims 77-82 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 77, as amended, recites:

> 77. The method for securely providing a subscriber of a subscriber network with an encrypted program, wherein the encrypted program includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving a first ciphertext packet of the encrypted program;
>
> ***applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> transmitting the second ciphertext packet.

(Emphasis added).

Applicant respectfully submits that claim 77 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a

claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 77 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 77, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 77 is allowable over the cited references of record, dependent claims 78-82 (which depend from independent claim 77) are allowable as a matter of law for at least the reason that dependent claims 78-82 contain all the features of

independent claim 77. Therefore, the rejection to claims 78-82 should be withdrawn and the claims allowed.

G. Claims 83-91

The Office Action rejects claims 83-91 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 83, as amended, recites:

> 83 A receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon;
>
> a key generator adapted to generate an encryption key; and
>
> ***a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet***.

(Emphasis added).

Applicant respectfully submits that claim 83 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 83 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 83, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 83 is allowable over the cited references of record, dependent claims 84-91 (which depend from independent claim 83) are allowable as a matter of law for at least the reason that dependent claims 84-91 contain all the features of

independent claim 83. Therefore, the rejection to claims 84-91 should be withdrawn and the claims allowed.

H. Claims 92-99

The Office Action rejects claims 92-99 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 92, as amended recites:

> 92. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using a first key;
>
> generating a second and third key;
>
> ***applying to the first ciphertext packet a second cryptographic algorithm with the second key to convert the first ciphertext packet to a second ciphertext packet having a second layer of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> applying to the second ciphertext packet a third cryptographic algorithm with the third key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

(Emphasis added).

Applicant respectfully submits that claim 92 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a

claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 92 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying to the first ciphertext packet a second cryptographic algorithm with the second key to convert the first ciphertext packet to a second ciphertext packet having a second layer of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 92, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 92 is allowable over the cited references of record, dependent claims 93-99 (which depend from independent claim 92) are allowable as a matter of law for at least the reason that dependent claims 93-99 contain all the features of

independent claim 92. Therefore, the rejection to claims 93-99 should be withdrawn and the claims allowed.

I. Claims 100-104

The Office Action rejects claims 100-104 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 100, as amended, recites:

100. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
an input port adapted to receive a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using a first key;
a key generator adapted to generate a plurality of keys including a second key and a third key;
a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet, without first converting the first ciphertext packet received from the headend to a cleartext packet, using a second cryptographic algorithm and the second key and thereafter to convert the second ciphertext packet to a third ciphertext packet, without first converting the second ciphertext packet to a cleartext packet, using a third cryptographic algorithm and the third key; and
a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second and third keys.

(Emphasis added).

Applicant respectfully submits that claim 100 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection

of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 100 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet, without first converting the first ciphertext packet received from the headend to a cleartext packet, using a second cryptographic algorithm and the second key**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 100, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 100 is allowable over the cited references of record, dependent claims 101-104 (which depend from independent claim 100) are allowable as a matter of law for at least the reason that dependent claims 101-104 contain all the features of

independent claim 100. Therefore, the rejection to claims 101-104 should be withdrawn and the claims allowed.

J. Claims 105-109

The Office Action rejects claims 105-109 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 105, as amended, recites:

> 105. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, the second key and the third key;
>
> generating a fourth key;
>
> ***applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

(Emphasis added).

Applicant respectfully submits that claim 105 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection

of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 105 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 105, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 105 is allowable over the cited references of record, dependent claims 106-109 (which depend from independent claim 105) are allowable as a matter of law for at least the reason that dependent claims 106-109 contain all the features of

independent claim 105. Therefore, the rejection to claims 106-109 should be withdrawn and the claims allowed.

K. Claims 110-114

The Office Action rejects claims 110-114 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 110, as amended, recites:

> 110. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key;
>
> a key generator adapted to generate a fourth key;
>
> ***a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet*** and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet; and
>
> a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys.

(Emphasis added).

Applicant respectfully submits that claim 110 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection

of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 110 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 110, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 110 is allowable over the cited references of record, dependent claims 111-114 (which depend from independent claim 110) are allowable as a matter of law for at least the reason that dependent claims 111-114 contain all the features of

independent claim 110. Therefore, the rejection to claims 111-114 should be withdrawn and the claims allowed.

L. Claims 115-119

The Office Action rejects claims 115-119 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 115, as amended, recites:

> 115. A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:
>
> receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key and a second key, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
>
> generating a third key; and
>
> ***applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet.***

(Emphasis added).

Applicant respectfully submits that claim 115 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 115 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 115, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 115 is allowable over the cited references of record, dependent claims 116-119 (which depend from independent claim 115) are allowable as a matter of law for at least the reason that dependent claims 116-119 contain all the features of independent claim 115. Therefore, the rejection to claims 116-119 should be withdrawn and the claims allowed.

M. Claims 120-124

The Office Action rejects claims 120-124 under 35 U.S.C. §103(a) as allegedly being unpatentable over *Rabowsky* (U.S. Patent No. 6,141,530) in view of *Stallings*, "Cryptography and Network Security, Principles and Practice," Second Edition, 1999. For at least the reasons set forth below, Applicant respectfully traverses the rejection.

Independent claim 120, as amended, recites:

> 120. A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:
>
> an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;
>
> a key generator adapted to generate a third key;
>
> ***a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet***; and
>
> a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the first, second and third keys.

(Emphasis added).

Applicant respectfully submits that claim 120 patently defines over the cited art for at least the reason that the cited art does not disclose the features emphasized above. For a proper rejection of a claim under 35 U.S.C. §103, the cited combination of references must disclose, teach, or suggest all elements/features of the claim at issue.

Applicant respectfully submits that independent claim 120 is allowable for at least the reason that the combination of *Rabowsky* and *Stallings* does not disclose, teach, or suggest at least **a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet**. Even if, assuming for the sake of argument, *Rabowsky* applies a 3DES encryption algorithm to a video stream, *Rabowsky* fails to disclose receiving a ciphertext packet from the headend/input port and applying at least one further cryptographic algorithm to the ciphertext packet that was received from the headend without first decrypting the ciphertext packet to a cleartext packet. In *Rabowsky*, each step of the 3DES encryption is resident on the receiver. Conversely, in at least one embodiment of the instant claim, the first encryption step is performed before the packet is received and the remaining encryption step(s) is (are) performed after the packet is received. In at least one embodiment, this results in a lighter processing load on the receiver, which might be a set top box, among other embodiments. *Stallings* does not cure this deficiency. As the cited combination of references does not disclose, teach, or suggest, either implicitly or explicitly, all the elements of claim 120, the rejection should be withdrawn for at least that reason.

For at least the reason that independent claim 120 is allowable over the cited references of record, dependent claims 121-124 (which depend from independent claim 120) are allowable as a matter of law for at least the reason that dependent claims 121-124 contain all the features of independent claim 120. Therefore, the rejection to claims 121-124 should be withdrawn and the claims allowed.

III. Miscellaneous Issues

Any other statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and official notice, or statements interpreted similarly, should not be considered well known for at least the specific and particular reason that the Office Action does not include specific factual findings predicated on sound technical and scientific reasoning to support such conclusions.

CONCLUSION

For at least the reasons set forth above, Applicant respectfully submits that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the now pending claims 1-124 are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

It is believed that no extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to deposit account No. 20-0778.

Respectfully submitted,

/BAB/

Benjamin A. Balser, Reg. No. 58,169

THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500